# On the Peak-to-Mean Envelope Power Ratio of Phase-Shifted Binary Codes

Kai-Uwe Schmidt



**Abstract**

The peak-to-mean envelope power ratio (PMEPR) of a code employed in orthogonal frequency-division multiplexing (OFDM) systems can be reduced by permuting its coordinates and by rotating each coordinate by a fixed phase shift. Motivated by some previous designs of phase shifts using suboptimal methods, the following question is considered in this paper. For a given binary code, how much PMEPR reduction can be achieved when the phase shifts are taken from a $2^h$-ary phase-shift keying ($2^h$-PSK) constellation? A lower bound on the achievable PMEPR is established, which is related to the covering radius of the binary code. Generally speaking, the achievable region of the PMEPR shrinks as the covering radius of the binary code decreases. The bound is then applied to some well understood codes, including nonredundant BPSK signaling, BCH codes and their duals, Reed–Muller codes, and convolutional codes. It is demonstrated that most (presumably not optimal) phase-shift designs from the literature attain or approach our bound.

**Index Terms**

BCH codes, convolutional codes, covering radius, orthogonal frequency-division multiplexing (OFDM), peak-to-average power ratio (PAPR), peak-to-mean envelope power ratio (PMEPR), Reed–Muller codes

## I. Introduction

Orthogonal frequency-division multiplexing (OFDM), a special kind of multicarrier communications, is a key concept in the development of wired and wireless communications systems in the past decade. It provides excellent ability to cope with multipath propagation and fast-moving environment. On the other hand, a principal drawback of OFDM is the typically high peak-to-mean envelope power ratio (PMEPR) of uncoded OFDM signals. That is, the peak transmit power can be many times the average transmit power.

Kai-Uwe Schmidt is with Communications Laboratory, Dresden University of Technology, 01062 Dresden, Germany, e-mail: schmidtk@ifn.et.tu-dresden.de, web: http://www.ifn.et.tu-dresden.de/∼schmidtk/

In order to ensure a distortionless transmission, all components in the transmission chain must be linear across a wide range of signal levels. This makes the transmitter considerably more expensive than one in a single-carrier system. Moreover, most of the time, the components in the transmitter are operated at levels much below their maximum input level, which results in power inefficiency. The latter issue is particularly acute in mobile applications, where battery lifetime is a major concern. On the other hand, nonlinearities in the transmission chain may lead to a loss of orthogonality among the carriers and to out-of-band radiation. The former has the effect of degrading the total system performance and the latter is subject to strong regulations.

Among various approaches to solve this power-control problem, the use of block coding across the carriers [16] combined with error protection [15] is one of the most promising concepts [22]. Here the goal is to design error-correcting codes that contain only codewords with low PMEPR.

A simple approach for the design of such codes was originally proposed by Jones and Wilkinson [15] and further developed by Tarokh and Jafarkhani [26]. The idea is to take a well understood code and to rotate each coordinate of the code by a fixed phase shift such that the maximum PMEPR taken over all codewords is minimized. This modification leaves unchanged the rate and the error-correcting properties of the code. Moreover a standard decoder for the original code can be employed in the receiver upon back rotation of the phase shifts.

Unfortunately, except perhaps for very short codes, the computation of the optimal phase shifts (which minimize the PMEPR) is considered to be extremely difficult and a feasible solution is unknown. Several suboptimal algorithms have been proposed in the literature [15], [26], [29]. These techniques were applied to obtain phase shifts for short Hamming codes [15], convolutional codes [26], [29], and nonredundant signaling [29]. However the achieved PMEPR reductions are rather small. One reason for this may be the suboptimality of the employed algorithms: the use of suboptimal techniques generally results in the convergence of the algorithm to a local minimum, and therefore, it is never certain that the optimal phase shifts are computed.

In this paper we study the fundamental limit of the achievable PMEPR of phase-shifted binary codes. We prove a lower bound for this limit and try to answer the question whether suboptimal phase-shift-design algorithms reported in the literature are in principle useful to approach this limit. The bound can be used to estimate the gap between the reduced PMEPR, obtained using suboptimal methods, and the global minimum. This allows us, in many cases, to establish the (near) optimality of some known phase-shift designs. We will also see that for several codes of practical importance a significant PMEPR reduction is ruled out by our results.

An outline of the remainder of this paper is given below. In the next section we introduce a simple OFDM model and state the problem formally. This involves a quantization of the phase shifts such that the phase-shifted code is a $2^h$-ary phase-shift keying ($2^h$-PSK) code. Theorem 2

in Section III states a lower bound on the PMEPR of such codes. The general case, where the restriction on the phase shifts is dropped, is then recovered in Corollary 3 by analyzing this bound for $h \to \infty$. The implication of this result for several codes, including nonredundant BPSK signaling, BCH codes and their duals, Reed–Muller codes, and convolutional codes, is discussed in Section IV. Section V contains the proofs of our main results. In Section VI we close with some concluding remarks and a brief discussion of open problems.

## II. Problem Statement

Consider a code $\mathcal{C} \subseteq \mathbb{Z}_{2^h}^n$, and let $c = (c_0, \ldots, c_{n-1})$ be a codeword in $\mathcal{C}$. The element $c_i$ is referred to as the $i$th *coordinate* of $\mathcal{C}$. With any $c$ we associate another word $\hat{c} = (\hat{c}_0, \ldots, \hat{c}_{n-1})$, where $\hat{c}_i = e^{j2\pi c_i/2^h}$ and $j$ is an imaginary unit such that $j^2 = -1$. Then $\{\hat{c} \,|\, c \in \mathcal{C}\}$ is a $2^h$-PSK code. Given a codeword $c \in \mathcal{C}$, the transmitted OFDM signal is the real part of the *complex envelope*, which can be written as

$$S_c(\theta) = \sum_{i=0}^{n-1} \hat{c}_i \, e^{j2\pi(i+\zeta)\theta}, \qquad 0 \le \theta < 1, \tag{1}$$

where $\zeta$ is a positive constant. Note that the guard interval is omitted in our model since it does not affect the PMEPR of the signal. Moreover our model only considers codes defined over PSK constellations.

The signal $|S_c(\theta)|^2$, which is independent of $\zeta$, is called the *instantaneous envelope power* of $S_c(\theta)$. It is a consequence of Parseval's identity that the mean value of $|S_c(\theta)|^2$ is equal to $||\hat{c}||^2 = \sum_{i=0}^{n-1} |\hat{c}_i|^2 = n$. Therefore the PMEPR of the word $c$ (or of the signal $S_c(\theta)$) is given by

$$\text{PMEPR}(c) := \frac{1}{n} \sup_{0 \le \theta < 1} |S_c(\theta)|^2. \tag{2}$$

Occasionally we shall indicate the PMEPR of $c$ as $10 \cdot \log_{10} \text{PMEPR}(c)$ [dB]. The PMEPR of the code $\mathcal{C}$ is now defined to be

$$\text{PMEPR}(\mathcal{C}) := \max_{c \in \mathcal{C}} \text{PMEPR}(c).$$

Observe that $\text{PMEPR}(\mathcal{C})$ can be as much as $n$, which occurs, for example, if $\mathcal{C}$ contains a constant codeword. Hence the PMEPR of every linear code is equal to $n$.

The OFDM coding problem may now be stated as follows. Design codes of length $n$ with high rate, large minimum distance, and PMEPR significantly lower than $n$. This problem is considered to be difficult, and only a few explicit constructions are known [22], [9], [21], [23], [24]. An even more challenging problem is the construction of sequences of codes with increasing length $n$, nonvanishing rate, and PMEPR growing strictly slower than linearly in $n$. Some results on the existence of such codes have been established in [22], [25].

The following approach for designing codes with reduced PMEPR was originally proposed by Jones and Wilkinson [15].

Let $\mathcal{B} \subseteq \mathbb{Z}_2^n$ be a binary code. We say that a code $\mathcal{C} \subseteq \mathbb{Z}_{2^h}^n$ is *equivalent* to $\mathcal{B}$ if there exists a permutation $\sigma$ of $\{0, 1, \ldots, n-1\}$ and an offset $w \in \mathbb{Z}_{2^h}^n$ such that

$$\mathcal{C} = \left\{ 2^{h-1}\sigma(b) + w \,|\, b \in \mathcal{B} \right\},$$

where we write $\sigma(b)$ in place of $(b_{\sigma(0)}, \ldots, b_{\sigma(n-1)})$. Note that, if $h = 1$ and $\mathcal{B}$ is linear, $\mathcal{C}$ is permutation equivalent to a coset of $\mathcal{B}$.

The $2^h$-PSK code corresponding to $\mathcal{C}$ is given by

$$\left\{ \hat{b}_{\sigma(0)} e^{j2\pi w_0/2^h}, \ldots, \hat{b}_{\sigma(n-1)} e^{j2\pi w_{n-1}/2^h} \;\middle|\; b \in \mathcal{B} \right\}.$$

Such a code is a *phase-shifted version* of a code that is permutation equivalent to the BPSK code associated with $\mathcal{B}$, where the $i$th phase shift is equal to $2\pi w_i/2^h$ with $w_i \in \mathbb{Z}_{2^h}$. Notice that, when $h$ tends to infinity, any phase shift can be approximated in this way with arbitrarily high precision.

Now let $E_h(\mathcal{B})$ be the set of all codes $\mathcal{C} \subseteq \mathbb{Z}_{2^h}^n$ that are equivalent to $\mathcal{B}$. By $E_\infty(\mathcal{B})$ we denote the infinite set $E_h(\mathcal{B})$ when $h$ tends to infinity (that is, the codes in $E_\infty(\mathcal{B})$ are defined over the 2-adic integers $\mathbb{Z}_{2^\infty}$). Any code in $E_h(\mathcal{B})$ has the same error-correcting capability and the same rate as $\mathcal{B}$, but the PMEPR of a particular $\mathcal{C} \in E_h(\mathcal{B})$ may be much lower than that of $\mathcal{B}$.

The power-control problem for OFDM can now be tackled as follows. Given a positive integer $h$ and a good (in the classical coding-theoretic sense) binary error-correcting code $\mathcal{B}$, find a code in $E_h(\mathcal{B})$ whose PMEPR is equal to

$$\min_{\mathcal{C} \in E_h(\mathcal{B})} \text{PMEPR}(\mathcal{C}). \tag{3}$$

This problem is considered to be extremely difficult, and only suboptimal algorithms are known, which may not even find a code whose PMEPR is close to the preceding expression. In this light we ask: what is the value of (3)? A lower bound for this quantity will be stated in the next section.

We remark that, although (3) is a nonincreasing function of $h$, in practice, $h$ is typically small, say 2 or 3, in order to allow efficient hardware implementation.

## III. Main Result

Recall that the *Hamming weight*, $\text{wt}_H(b)$, of a binary vector $b$ is equal to the number of nonzero elements in $b$. Our lower bound for (3) will be expressed in terms of the covering radius of the binary code $\mathcal{B}$, which is defined below.

*Definition 1:* The *covering radius* of a code $\mathcal{B} \subseteq \mathbb{Z}_2^n$ is defined to be

$$\rho(\mathcal{B}) := \max_{x \in \mathbb{Z}_2^n} \min_{b \in \mathcal{B}} \mathrm{wt}_H(b + x).$$

In words, $\rho(\mathcal{B})$ is the least nonnegative integer such that the spheres of radius $\rho(\mathcal{B})$ around the codewords of $\mathcal{B}$ cover the space $\mathbb{Z}_2^n$. If $\mathcal{B}$ is linear, $\rho(\mathcal{B})$ is equal to the maximum weight of the coset leaders of $\mathcal{B}$. Determining the covering radius of a binary code is generally nontrivial [18]. In spite of this, many results are known. For a good overview we refer to [7] and [3].

Once and for all we fix the following parameters depending on $h$:

$$\lambda := \begin{cases} 1 & \text{if} \quad h = 1 \\ 2 & \text{if} \quad h > 1 \end{cases}$$

and

$$\epsilon := \begin{cases} 1 & \text{if} \quad h = 1 \\ 2^{2h-3} \sin^2\left(\frac{\pi}{2^h}\right) & \text{if} \quad h > 1. \end{cases}$$

We are now in a position to state our main result, whose proof can be found in Section V.

*Theorem 2:* Given a binary code $\mathcal{B} \subseteq \mathbb{Z}_2^n$ with covering radius

$$\rho(\mathcal{B}) \leq n \left( \frac{1}{\epsilon} - \frac{1}{2} \right),$$

we have

$$\min_{\mathcal{C} \in E_h(\mathcal{B})} \mathrm{PMEPR}(\mathcal{C}) \geq \frac{1}{\lambda n} \left[ n(2 - \epsilon) - 2\,\epsilon\,\rho(\mathcal{B}) \right]^2.$$

The preceding lower bound is a decreasing function of $h$. However this decrease is bounded, and the corollary below states the asymptotic lower bound for $h \to \infty$.

*Corollary 3:* Let $\mathcal{B} \subseteq \mathbb{Z}_2^n$ be a binary code with covering radius

$$\rho(\mathcal{B}) \leq n \left( \frac{8}{\pi^2} - \frac{1}{2} \right).$$

Then

$$\min_{\mathcal{C} \in E_\infty(\mathcal{B})} \mathrm{PMEPR}(\mathcal{C}) \geq \frac{1}{2n} \left( n \frac{16 - \pi^2}{8} - \frac{\pi^2}{4} \rho(\mathcal{B}) \right)^2.$$

*Proof:* Recall that $\lambda = 2$ for any $h > 1$, and with the Taylor series

$$\sin^2 x = x^2 + O(x^4) \tag{4}$$

we conclude

$$\lim_{h \to \infty} \epsilon = \lim_{h \to \infty} 2^{2h-3} \sin^2\left(\frac{\pi}{2^h}\right) = \frac{\pi^2}{8}.$$

The corollary is then immediate. □

We note that the condition $\rho(\mathcal{B}) \leq n/2$ (which is for $h > 2$ slightly stronger than those in Theorem 2 and Corollary 3) is always met if $\mathcal{B}$ has strength 1 [7], [3], that is, each coordinate of $\mathcal{B}$ takes the values '0' and '1' equally often. In particular every linear code without a coordinate that is always zero has strength 1.

We conclude from Theorem 2 that a necessary condition to obtain a code over $\mathbb{Z}_{2^h}$ with low PMEPR from a binary code is that the covering radius of the underlying binary code must be larger than a certain threshold. More specifically, to obtain a sequence of codes with PMEPR growth strictly less than order $n$ from a sequence of binary codes, the covering radius of the binary code must grow when $n$ increases. In particular, in order to achieve a constant PMEPR, the covering radius of the binary code $\mathcal{B}$ must satisfy

$$\rho(\mathcal{B}) \geq n\left(\frac{1}{\epsilon} - \frac{1}{2}\right) - O(\sqrt{n}),$$

which can be replaced by the slightly stronger condition

$$\rho(\mathcal{B}) \geq \frac{n}{2} - O(\sqrt{n}). \tag{5}$$

We shall see in the next section that the preceding condition is satisfied for the duals of binary primitive BCH codes and for $r$th-order Reed–Muller codes. On the other hand, we will also see that Theorem 2 implies that the phase-shifted versions of many other codes have PMEPR growing linearly in $n$.

## IV. Implications

### A. Nonredundant BPSK Signaling

Consider the code $\mathbb{Z}_2^n$. The associated PSK code is a BPSK code without redundancy. Since $\rho(\mathbb{Z}_2^n) = 0$, Theorem 2 and Corollary 3 imply the following.

*Corollary 4:* For $h > 1$ we have

$$\min_{\mathcal{C} \in E_h(\mathbb{Z}_2^n)} \text{PMEPR}(\mathcal{C}) \geq \frac{(2-\epsilon)^2}{2} \cdot n$$

and

$$\min_{\mathcal{C} \in E_\infty(\mathbb{Z}_2^n)} \text{PMEPR}(\mathcal{C}) \geq 2n\left(1 - \frac{\pi^2}{16}\right)^2 \approx 0.2936 \cdot n.$$

In [29] Wunder and Boche proposed to use Newman phases [20] to reduce the PMEPR for nonredundant BPSK signaling. Newman phases are given by

$$\varphi_i = \frac{\pi i^2}{n}, \quad i = 0, 1, \ldots, n-1.$$

Applying the phase shift $\varphi_i$ to the $i$th coordinate of a BPSK code, we obtain a PSK code whose underlying code over $\mathbb{Z}_{2^\infty}$ is equivalent to $\mathbb{Z}_2^n$.

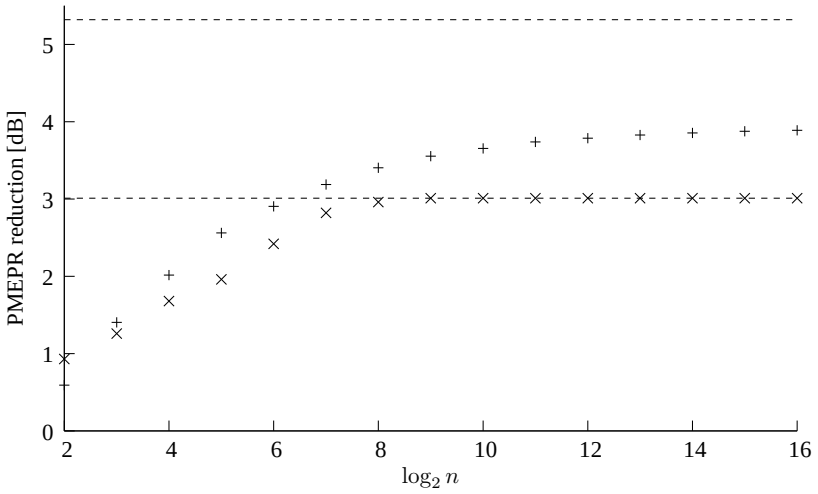


Fig. 1. PMEPR reduction for nonredundant BPSK signaling and $n$ carriers with Newman phases ($+$) and with Newman phases rounded to points in a QPSK constellation ($\times$), upper bounds (dashed lines)

For $n = 16$ and $n = 128$ in [29] the PMEPR could be reduced in this way from $12.04$ dB and $21.07$ dB to $9.97$ dB and $17.89$ dB, respectively. We have used the algorithm described in [29] to calculate the PMEPR reductions for lengths $n = 2^m$, where $m$ ranges from $2$ to $16$. In addition we have rounded the Newman phases to the nearest points in $\{+1, +j, -1, -j\}$, i.e., the phase-shifted code is a QPSK code. The results are presented in Figure 1. The figure also shows the corresponding bounds on the PMEPR reductions obtained with Corollary 4 ($-10 \log_{10} 0.5 \approx 3.01$ dB for $h = 2$ and $-10 \log_{10} 0.2936 \approx 5.32$ dB for $h \to \infty$). By using rounded Newman phases the bound in Corollary 4 is attained for $m \geq 9$. With the original Newman phases the PMEPR reduction seems to converge to approximately $3.9$ dB. Thus for large $n$ Newman phases approach our bound by about $1.4$ dB.

### *B. Linear Codes*

Next we present a lower bound for the PMEPR of codes over $\mathbb{Z}_{2^h}$ that are equivalent to a given binary linear code as a function of the code rate.

*Corollary 5:* Let $\mathcal{B} \subseteq \mathbb{Z}_2^n$ be a binary linear code with rate

$$R \geq \frac{3}{2} - \frac{1}{\epsilon}.$$

Then

$$\min_{\mathcal{C} \in E_h(\mathcal{B})} \text{PMEPR}(\mathcal{C}) \geq \frac{4n}{\lambda} \left[ 1 - \epsilon \left( \frac{3}{2} - R \right) \right]^2.$$

*Proof:* Let $k$ be the dimension of $\mathcal{B}$ such that $R = k/n$. The redundancy bound [7], [3] states

$$\rho(\mathcal{B}) \leq n - k. \tag{6}$$

The condition $k/n \geq 3/2 - 1/\epsilon$ then implies that

$$\rho(\mathcal{B}) \leq n\left(\frac{1}{\epsilon} - \frac{1}{2}\right).$$

Hence we can plug (6) into the inequality in Theorem 2, which yields the desired expression. □

The above corollary shows explicitly that it is impossible to construct a sequence of codes over $\mathbb{Z}_{2^h}$ from a sequence of binary linear codes with rate $R > 3/2 - 1/\epsilon$ and PMEPR growth slower than linear in $n$.

We remark that some improved bounds for linear codes can be obtained by taking bounds for the covering radius that are better than the redundancy bound, e.g., the Griesmer-like upper bound on the covering radius of linear codes [14], which takes the minimum distance of the code into account.

### *C. Binary Primitive BCH Codes and Their Duals*

In what follows we will analyze lower bounds on the PMEPR of codes that are equivalent to binary primitive $t$-error-correcting BCH codes, $\mathcal{B}(t, m)$, and their duals, $\mathcal{B}^{\perp}(t, m)$. These codes have length $2^m - 1$. See, e.g., [17] for details on these codes.

*Corollary 6:* Let $n = 2^m - 1$. Then we have

$$\min_{\mathcal{C} \in E_h(\mathcal{B}(t,m))} \text{PMEPR}(\mathcal{C}) \geq \frac{1}{\lambda n}[n(2-\epsilon) - \epsilon(4t-2)]^2$$

for $t = 1$, $m \geq 2$ , for $t = 2$, $m \geq 3$, for $t = 3$, $m \geq 4$, and for arbitrary $t$ and $m \geq m_0$, where $m_0$ is finite and depends on $t$.

*Proof:* It is known that $\rho(\mathcal{B}(1, m)) = 1$ for $m \geq 2$ ($\mathcal{B}(1, m)$ is perfect), $\rho(\mathcal{B}(2, m)) = 3$ for $m \geq 3$ [11], $\rho(\mathcal{B}(3, m)) = 5$ for $m \geq 4$ [12]. More generally, it was proved in [28] that there exists an $m_0$ depending on $t$ such that $\rho(\mathcal{B}(t, m)) = 2t - 1$ for all $m \geq m_0$. Putting these values into Theorem 2 yields the statement in the corollary. □

*Remark:* It has been shown in [8] that $m_0$ satisfies

$$m_0 \leq 2\log_2\left[(2t-1)!\,(2t-3)\right].$$

The preceding corollary shows that every code in $E_h(\mathcal{B}(t, m))$ has PMEPR growing linearly in $n$.

Jones and Wilkinson [15] applied a learning algorithm to obtain phase shifts for $\mathcal{B}(1,3)$ and $\mathcal{B}(1,4)$, the first nontrivial Hamming codes. As a result, [15] reports binary phases that reduce the PMEPR from $8.45$ dB and $11.76$ dB to $5.53$ dB and $10.52$ dB, respectively. These values meet the lower bound in Corollary 6, and we conclude that the binary phase shifts computed in [15] are the best possible. In [15] the learning algorithm was also applied to find offsets over $\mathbb{Z}_8$. The respective reduced PMEPRs are $3.42$ dB and $8.47$ dB. For $\mathcal{B}(1,3)$ Corollary 6 fails to provide a nontrivial lower bound. For $\mathcal{B}(1,4)$ Corollary 6 yields the lower bound $5.30$ dB.

Let us turn our attention to $\mathcal{B}^{\perp}(t,m)$.

*Corollary 7:* Let $n = 2^m - 1$. Then

$$\min_{\mathcal{C} \in E_1(\mathcal{B}^{\perp}(t,m))} \text{PMEPR}(\mathcal{C}) \geq \frac{1}{n}\left[1 + 2(\sqrt{t} - \sqrt[6]{t})\sqrt{n-t-1}\right]^2.$$

*Proof:* The corollary follows from Theorem 2 and a result from [27]

$$\rho(\mathcal{B}^{\perp}(t,m)) \leq \frac{n-1}{2} - (\sqrt{t} - \sqrt[6]{t})\sqrt{n-t-1}.$$

□

Observe that the covering radius of $\mathcal{B}^{\perp}(t,m)$ satisfies (5), and the lower bound on the PMEPR is asymptotically independent of the code length. However notice that the rate is strictly decreasing with increasing length. It is noteworthy that Paterson and Tarokh [22] obtained a bound on the PMEPR of the nonzero codewords of $\mathcal{B}^{\perp}(t,m)$, which has order $(\log n)^2$, and they speculated that by taking cosets of $\mathcal{B}^{\perp}(t,m)$ the PMEPR may be significantly further reduced. This conjecture is supported by Corollary 7.

### *D. Reed–Muller Codes*

Next we establish lower bounds on the PMEPR of codes that are equivalent to $r$th-order Reed–Muller codes of length $2^m$, $\text{RM}(r,m)$. See, e.g., [17] for details on these codes. For $r = 1$ we have the following.

*Corollary 8:* The PMEPR of any code in $E_1(\text{RM}(1,m))$ is at least 2 for odd $m \leq 7$ and is lower bounded by 1 in all other cases.

*Proof:* It was proved in [13] that

$$2^{m-1} - 2^{(m-1)/2} \leq \rho(\text{RM}(1,m)) \leq 2^{m-1} - 2^{m/2-1}, \tag{7}$$

where the upper bound is tight when $m$ is even. The lower bound of 1 for the PMEPR follows then from Theorem 2 (for odd $m$ the lower bound can be tightened slightly by taking into account that $\rho(\text{RM}(1,m))$ must be an integer). In the special case where $m$ is odd and $m \leq 7$ it is known that the lower bound in (7) is tight [1], [19]. Therefore Theorem 2 states that the PMEPR is lower bounded by 2 in this case. □

Indeed Davis and Jedwab [9] explicitly constructed $m!/2$ binary offsets for $\mathrm{RM}(1,m)$ that reduce the PMEPR to values not exceeding $2$ for any $m$. Hence the bound in Corollary 8 is attained for odd $m \leq 7$.

Corollary 8 only considers the case when $h = 1$. However, even if $\rho(\mathrm{RM}(1,m))$ attains the lower bound in (7), Theorem 2 yields the trivial lower bound 1 for the PMEPR of quaternary codes equivalent to $\mathrm{RM}(1,m)$ for all choices of $m$.

Let us turn our attention to Reed–Muller codes of arbitrary order. For $r > 1$ general explicit results for the covering radius of $\mathrm{RM}(r,m)$ are unknown. For small $r$ and $m$ a few values and bounds are given in [3, page 802]. However good asymptotic bounds are known, which enable us to analyze the asymptotic behavior of Theorem 2 for all Reed–Muller codes of fixed order. Previous asymptotic bounds for $\rho(\mathrm{RM}(r,m))$ ($r > 1$) have been recently improved in [6] to

$$\rho(\mathrm{RM}(r,m)) \leq 2^{m-1} - \frac{\sqrt{15}}{2}\left(\sqrt{2}+1\right)^{r-2} \cdot 2^{m/2} + O(1).$$

Observe that the covering radius satisfies (5). Hence for fixed $r$ Theorem 2 yields a lower bound that is asymptotically a constant. More specifically, we obtain the following.

*Corollary 9:* When $m$ tends to infinity, we have

$$\min_{\mathcal{C} \in E_1(\mathrm{RM}(r,m))} \mathrm{PMEPR}(\mathcal{C}) \geq 15\left(\sqrt{2}+1\right)^{2r-4}$$

for $r > 1$.

This bound is indeed independent of the length of the code. But notice that for fixed $r$ the code rate tends to zero as the length of the code increases.

### *E. Convolutional Codes*

Consider a convolutional encoder with $k_0$ binary inputs, $n_0$ binary outputs, and constraint length $\nu + 1$. Suppose that the initial state of the encoder is arbitrary. The corresponding convolutional code consists of all possible output sequences of infinite length. The set of all binary output sequences of length $\ell n_0$ may be viewed as a linear block code $\mathcal{C}_\ell$ with generator matrix

$$\begin{pmatrix}
g_\nu & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 \\
g_{\nu-1} & g_\nu & \cdots & 0 & 0 & 0 & \cdots & 0 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
g_0 & g_1 & \cdots & g_\nu & 0 & 0 & \cdots & 0 \\
0 & g_0 & \cdots & g_{\nu-1} & g_\nu & 0 & \cdots & 0 \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
0 & 0 & \cdots & 0 & 0 & 0 & \cdots & g_0
\end{pmatrix},$$

where $g_0, g_1, \ldots, g_\nu$ are matrices of size $k_0 \times n_0$ with elements in $\mathbb{Z}_2$, and $0$ is the all-zero matrix of the same size. Then $\mathcal{C}_\ell$ has length $n = \ell n_0$ and dimension $k = (\ell+\nu)k_0$. Note that the first $\nu k_0$ information bits are fed into the encoder to produce the initial state. This situation corresponds to the case where a block of $\ell$ subsequent symbols of a continuous stream of encoder outputs is used as a binary codeword of length $\ell n_0$ to modulate one OFDM symbol. So the initial state of this block is the final state of the previous block.

The *normalized covering radius* of a convolutional code $\mathcal{C}$ is defined to be [2], [4]

$$\tilde{\rho}(\mathcal{C}) := \lim_{\ell \to \infty} \frac{\rho(\mathcal{C}_\ell)}{\ell n_0}.$$

Bounds for the normalized covering radius of some convolutional codes can be found in [2] and [4]. The covering radius of $\mathcal{C}_\ell$ satisfies [2]

$$\rho(\mathcal{C}_\ell) \leq n\, \tilde{\rho}(\mathcal{C}).$$

With Theorem 2 the next corollary is now immediate.

*Corollary 10:* With the notation as above, suppose that

$$\tilde{\rho}(\mathcal{C}) \leq \frac{1}{\epsilon} - \frac{1}{2}.$$

Then

$$\min_{\mathcal{D} \in E_h(\mathcal{C}_\ell)} \text{PMEPR}(\mathcal{D}) \geq \frac{4n}{\lambda} \left[ 1 - \epsilon \left( \tilde{\rho}(\mathcal{C}) + \frac{1}{2} \right) \right]^2.$$

The preceding corollary states that, whenever $\tilde{\rho}(\mathcal{C}) \leq 1/\epsilon - 1/2$, the PMEPR of any code in $E_h(\mathcal{C}_\ell)$ grows linearly in $n$. We remark that for a particular $n$ the result can be tightened slightly by taking into account that the covering radius of a block code of finite length must be an integer.

As an example let us consider the scenario of binary signaling in the HiPerLAN/2 OFDM system [10], which uses 48 carriers for data transmission. The employed convolutional code $\mathcal{C}$ is completely described by

$$(g_0, g_1, \ldots, g_6) = ((11), (01), (11), (11), (00), (10), (11)),$$

so $\nu = 6$, $k_0 = 1$, and $n_0 = 2$. Tarokh and Jafarkhani [26] have computed quaternary, octary, and $16$-ary phase shifts for $\mathcal{C}_{24}$ of length $48$. The respective reduced PMEPR is equal to $12.7$ dB, $12.6$ dB, and $12.4$ dB. We used a simple search algorithm in combination with the techniques reported in [29] to find a binary offset that reduces the PMEPR to $14.6$ dB. Notice that the PMEPR of the original code $\mathcal{C}_{24}$ is equal to $16.8$ dB since the code is linear and, therefore, contains the all-zero word.

From [2] we know that $\tilde{\rho}(\mathcal{C}) \leq 1/5$, therefore, $\rho(\mathcal{C}_{24}) \leq 9$. However direct computation yields $\rho(\mathcal{C}_{24}) = 6$. Applying Theorem 2 directly, the PMEPR of any code in $E_h(\mathcal{C}_{24})$ is at least $14.3$ dB, $11.3$ dB, $8.4$ dB, and $7.4$ dB for $h = 1, 2, 3, 4$, respectively. We conclude that for $h = 1$ a significant PMEPR reduction is precluded by our results and the reduced PMEPR approaches our bound by $0.3$ dB, for $h = 2$ the PMEPR reduction obtained in [26] is at least close to the best possible, and for $h = 3, 4$ the gap between the reduced PMEPR and our lower bound is about $4$–$5$ dB. This gap may have the following reasons: (i) Theorem 2 is not tight in this case, (ii) the optimization algorithm in [26] converged to a local minimum, or (iii) a lower PMEPR can be obtained by applying another permutation to the coordinates of the code.

## V. Proofs

### A. Proof of Theorem 2 When $h = 1$

Here $\lambda = 1$ and $\epsilon = 1$. Let $a = (a_0, \ldots, a_{n-1}) \in \mathbb{Z}_2^n$. From (2) and (1) we have

$$\begin{aligned}\text{PMEPR}(a) &\geq \frac{1}{n}|S_a(0)|^2 \\ &= \frac{1}{n}\left|\sum_{i=0}^{n-1}(-1)^{a_i}\right|^2 \\ &= \frac{1}{n}[n - 2\text{wt}_H(a)]^2.\end{aligned}$$

It follows that

$$\begin{aligned}\min_{\mathcal{C}\in E_1(\mathcal{B})} \text{PMEPR}(\mathcal{C}) &= \min_{\sigma}\min_{w\in\mathbb{Z}_2^n}\max_{b\in\mathcal{B}} \text{PMEPR}(\sigma(b) + w) \\ &\geq \frac{1}{n}\min_{\sigma}\min_{w\in\mathbb{Z}_2^n}\max_{b\in\mathcal{B}}[n - 2\text{wt}_H(\sigma(b) + w)]^2 \\ &= \frac{1}{n}\min_{w\in\mathbb{Z}_2^n}\max_{b\in\mathcal{B}}[n - 2\text{wt}_H(b + w)]^2.\end{aligned}$$

The condition $\rho(\mathcal{B}) \leq n/2$ implies that $n - 2\rho(\mathcal{B})$ is nonnegative. Therefore we arrive at

$$\begin{aligned}\min_{\mathcal{C}\in E_1(\mathcal{B})} \text{PMEPR}(\mathcal{C}) &\geq \frac{1}{n}[n - 2\max_{w\in\mathbb{Z}_2^n}\min_{b\in\mathcal{B}} \text{wt}_H(b + w)]^2 \\ &= \frac{1}{n}[n - 2\rho(\mathcal{B})]^2,\end{aligned}$$

and the theorem follows for $h = 1$. □

*B. Proof of Theorem 2 When $h > 1$*

We need some preliminaries in order to set out the proof. The *Lee weight* of the word $a = (a_0, \ldots, a_{n-1}) \in \mathbb{Z}_{2^h}^n$ is defined to be

$$\mathrm{wt}_L(a) := \sum_{i=0}^{n-1} \min\left\{a_i, 2^h - a_i\right\}.$$

*Lemma 11:* For each $a, b \in \mathbb{Z}_{2^h}^n$ and $h > 1$ we have

$$||\hat{a} - \hat{b}||^2 \leq 2^h \sin^2\left(\frac{\pi}{2^h}\right) \mathrm{wt}_L(a - b).$$

*Proof:* It suffices to prove the lemma for $n = 1$. It is straightforward to establish that

$$\begin{aligned} ||\hat{a} - \hat{b}||^2 &= 4\sin^2\left((a-b)\frac{\pi}{2^h}\right) \\ &= 4\sin^2\left(\mathrm{wt}_L(a-b)\frac{\pi}{2^h}\right). \end{aligned}$$

Hence we have to show that

$$\sin^2\left(w\,\frac{\pi}{2^h}\right) \leq \frac{2^h}{4}\sin^2\left(\frac{\pi}{2^h}\right) w \tag{8}$$

holds for $h > 1$ and $w = 0, 1, \ldots, 2^{h-1}$. When $h = 2$, equality in (8) is easily proved by hand. For $h \geq 3$ the idea of the proof is as follows. Consider the function $f : \mathbb{R} \to \mathbb{R}$ with $f(x) = \sin^2(x\,\pi/2^h)$, which is a continuous equivalent of the LHS of (8). First a tangent to the curve $f(x)$ at some $0 < x_0 \leq 2^{h-1}$ is constructed that passes through the origin. Then it is shown that for $0 \leq x \leq 2^{h-1}$ and $h \geq 3$ the curve $f(x)$ is upper bounded by this tangent and the slope of this tangent is at most

$$\frac{2^h}{4}\sin^2\left(\frac{\pi}{2^h}\right), \tag{9}$$

which is the coefficient of $w$ in the RHS of (8).

The curve $f(x)$ has a local minimum at $x = 0$ and a local maximum at $x = 2^{h-1}$, and has exactly one inflection point between them. Since $x_0 > 0$, it is then obvious that the tangent must meet the curve $f(x)$ in the concave part at some $0 < x_0 \leq 2^{h-1}$, where $x_0$ is uniquely determined. We conclude that $f(x)$ is upper bounded by the tangent for $0 \leq x \leq 2^{h-1}$.

Since the tangent passes through the origin, $x_0$ must satisfy

$$f(x_0) = f'(x_0)x_0,$$

or equivalently,

$$\frac{2\pi x_0}{2^h} = \tan\left(\frac{\pi x_0}{2^h}\right). \tag{10}$$

Now we aim to show that $f'(x_0)$ is at most (9), which is equivalent to showing that

$$4\pi \sin\left(\frac{2\pi x_0}{2^h}\right) \leq 2^{2h} \sin^2\left(\frac{\pi}{2^h}\right), \tag{11}$$

where $x_0$ satisfies (10). Notice that (10) is a transcendental equation, which generally does not have a closed-form solution. However we can apply numerical methods to solve (10), and find that the LHS of (11) is upper bounded by $9.12$. The RHS of (11) is an increasing function in $h$, and by using (4), we conclude that when $h \to \infty$, it converges to $\pi^2$, clearly greater than $9.12$. Hence there exists an integer $h_0$ so that (11) is true for all $h \geq h_0$. Numerical analysis yields $h_0 = 3$. □

The following definition was mentioned in [5] as a generalization of the classical Gray map.

*Definition 12:* For any integer $h > 1$ we define the map $\phi : \mathbb{Z}_{2^h} \to \mathbb{Z}_2^{2^{h-1}}$ as follows. If $0 \leq a \leq 2^{h-1}$, the image $\phi(a)$ is the binary word $(000\cdots111)$ with Hamming weight equal to $a$. If $2^{h-1} < a < 2^h$, the image $\phi(a)$ is the binary word $(111\cdots000)$ with Hamming weight equal to $2^h - a$. We also define the maps $\beta, \gamma : \mathbb{Z}_{2^h} \to \mathbb{Z}_2^{2^{h-2}}$ such that for each $a \in \mathbb{Z}_{2^h}$

$$\phi(a) = (\beta(a), \gamma(a)).$$

Finally the maps $\phi$, $\beta$, and $\gamma$ are extended in the obvious way to act on words in $\mathbb{Z}_{2^h}^n$.

In the special case when $h = 2$, $\phi$ is the classical Gray map [5]. By virtue of its definition, $\phi$ is a weight-preserving map from $\mathbb{Z}_{2^h}^n$ supported by the Lee weight to $\mathbb{Z}_2^{2^{h-1}n}$ supported by the Hamming weight, i.e., for each $a \in \mathbb{Z}_{2^h}^n$ we have

$$\begin{aligned} \mathrm{wt}_L(a) &= \mathrm{wt}_H(\phi(a)) \\ &= \mathrm{wt}_H(\beta(a)) + \mathrm{wt}_H(\gamma(a)). \end{aligned}$$

We will need the following identities.

*Lemma 13:* For $a \in \mathbb{Z}_{2^h}^n$ and $b \in \mathbb{Z}_2^n$ we have

$$\begin{aligned} &(i) \quad \beta(a - 2^{h-2}) = \overline{\gamma(a)}, \quad \gamma(a - 2^{h-2}) = \beta(a) \\ &(ii) \quad \beta(a + 2^{h-1}b) = \beta(a) + \beta(2^{h-1}b), \end{aligned}$$

where the addition of scalars is understood to be componentwise, and $\overline{\gamma(a)}$ denotes the complement of $\gamma(a)$.

*Proof:* The statements in the lemma are immediate consequences of the apparent fact that for $a, \delta \in \mathbb{Z}_{2^h}$ the binary word $\phi(a + \delta)$ is equal to a negacyclic shift by $\delta$ positions to the left of the binary word $\phi(a)$. □

We are now in a position to complete the proof of Theorem 2.

*Proof of Theorem 2 When $h > 1$:* Now we have $\lambda = 2$ and $\epsilon = 2^{2h-3}\sin^2(\pi/2^h)$. Let $a = (a_0, \ldots, a_{n-1}) \in \mathbb{Z}_{2^h}^n$. It follows from (2) and (1) that

$$\begin{aligned}\text{PMEPR}(a) &\geq \frac{1}{n}\left|S_a(0)\right|^2 \\ &= \frac{1}{n}\left|\sum_{i=0}^{n-1}\hat{a}_i\right|^2.\end{aligned}$$

Using the easily verified identities

$$\begin{aligned}||\hat{a}-1||^2 &= 2n - 2\Re\left\{\sum_{i=0}^{n-1}\hat{a}_i\right\} \\ ||\hat{a}-j||^2 &= 2n - 2\Im\left\{\sum_{i=0}^{n-1}\hat{a}_i\right\},\end{aligned}$$

where we interpret the addition of scalars to sequences componentwise, we obtain

$$\text{PMEPR}(a) \geq \frac{1}{n}\left[\left(n - \frac{1}{2}||\hat{a}-1||^2\right)^2 + \left(n - \frac{1}{2}||\hat{a}-j||^2\right)^2\right].$$

The inequality

$$\begin{aligned}x^2 + y^2 &= \frac{1}{2}\left[(x+y)^2 + (x-y)^2\right] \\ &\geq \frac{1}{2}(x+y)^2, \quad x, y \in \mathbb{R}\end{aligned}$$

yields

$$\text{PMEPR}(a) \geq \frac{1}{2n}\left[2n - \frac{1}{2}\left(||\hat{a}-1||^2 + ||\hat{a}-j||^2\right)\right]^2.$$

Applying Lemma 11 we arrive at

$$\text{PMEPR}(a) \geq \frac{1}{2n}\left[2n - \frac{\epsilon}{2^{h-2}}\left(\text{wt}_L(a) + \text{wt}_L(a-2^{h-2})\right)\right]^2, \tag{12}$$

provided that the expression inside the square is nonnegative. This will be assumed in the following and justified at the end of the proof. We now use the weight-preserving property of the generalized Gray map $\phi$ (cf. Definition 12) and Lemma 13 (i) to establish

$$\begin{aligned}&\text{wt}_L(a) + \text{wt}_L(a-2^{h-2}) \\ &\quad= \text{wt}_H(\phi(a)) + \text{wt}_H(\phi(a-2^{h-2})) \\ &\quad= \text{wt}_H(\beta(a)) + \text{wt}_H(\gamma(a)) \\ &\qquad+ \text{wt}_H(\beta(a-2^{h-2})) + \text{wt}_H(\gamma(a-2^{h-2})) \\ &\quad= 2\text{wt}_H(\beta(a)) + \text{wt}_H(\gamma(a)) + \text{wt}_H(\overline{\gamma(a)}) \\ &\quad= 2\text{wt}_H(\beta(a)) + 2^{h-2}\,n,\end{aligned}$$

where $\overline{\gamma(a)}$ is the complement of $\gamma(a)$. Hence

$$\begin{aligned}\text{PMEPR}(a) &\geq \frac{1}{2n}\left[2n - \frac{\epsilon}{2^{h-2}}(2\text{wt}_H(\beta(a)) + 2^{h-2}n)\right]^2 \\ &= \frac{1}{2n}\left[n(2-\epsilon) - \frac{\epsilon}{2^{h-3}}\text{wt}_H(\beta(a))\right]^2.\end{aligned}$$

Indeed

$$\begin{aligned}&\min_{\mathcal{C}\in E_h(\mathcal{B})} \text{PMEPR}(\mathcal{C}) \\ &= \min_{\sigma}\min_{w\in\mathbb{Z}_{2^h}^n}\max_{b\in\mathcal{B}} \text{PMEPR}(2^{h-1}\sigma(b)+w) \\ &\geq \frac{1}{2n}\min_{\sigma}\min_{w\in\mathbb{Z}_{2^h}^n}\max_{b\in\mathcal{B}}\left[n(2-\epsilon) - \frac{\epsilon}{2^{h-3}}\,\text{wt}_H(\beta(w+2^{h-1}\sigma(b)))\right]^2 \\ &= \frac{1}{2n}\min_{w\in\mathbb{Z}_{2^h}^n}\max_{b\in\mathcal{B}}\left[n(2-\epsilon) - \frac{\epsilon}{2^{h-3}}\,\text{wt}_H(\beta(w+2^{h-1}b))\right]^2 \\ &= \frac{1}{2n}\min_{w\in\mathbb{Z}_{2^h}^n}\max_{b\in\mathcal{B}}\left[n(2-\epsilon) - \frac{\epsilon}{2^{h-3}}\,\text{wt}_H(\beta(w)+b')\right]^2,\end{aligned}$$

where Lemma 13 (ii) has been employed in the last step and $b'$ is given by

$$b' = \beta(2^{h-1}b) = (\underbrace{b\,b\,\cdots\,b}_{2^{h-2}\text{ times}}).$$

Recall that we imposed

$$\rho(\mathcal{B}) \leq n\left(\frac{1}{\epsilon} - \frac{1}{2}\right),$$

which implies that the expression $n(2-\epsilon) - 2\,\epsilon\,\rho(\mathcal{B})$ is nonnegative. Hence we can write

$$\begin{aligned}&\min_{\mathcal{C}\in E_h(\mathcal{B})} \text{PMEPR}(\mathcal{C}) \\ &\geq \frac{1}{2n}\min_{u\in\mathbb{Z}_2^{2^{h-2}n}}\max_{b\in\mathcal{B}}\left[n(2-\epsilon) - \frac{\epsilon}{2^{h-3}}\text{wt}_H(u+b')\right]^2 \\ &= \frac{1}{2n}\min_{u\in\mathbb{Z}_2^n}\max_{b\in\mathcal{B}}\left[n(2-\epsilon) - 2\,\epsilon\,\text{wt}_H(u+b)\right]^2 \\ &= \frac{1}{2n}\left[n(2-\epsilon) - 2\,\epsilon\max_{u\in\mathbb{Z}_2^n}\min_{b\in\mathcal{B}}\text{wt}_H(u+b)\right]^2 \\ &= \frac{1}{2n}\left[n(2-\epsilon) - 2\,\epsilon\,\rho(\mathcal{B})\right]^2.\end{aligned}$$

Since the terms inside the squares in the preceding expressions are nonnegative, our assumption leading to (12) holds, and the proof is completed. □

## VI. Conclusions and Open Problems

In this paper we have analyzed the reduction of the PMEPR of a code when a permutation and a fixed phase shift is applied to its coordinates. A lower bound on the PMEPR for the case where the phase shifts are quantized (i.e., they are in the set $\{2\pi i/2^h \,|\, i = 0, 1, \ldots, 2^h - 1\}$) was proved, and the asymptotic behavior for $h \to \infty$ was examined. The bound asserts that the achievable region of the PMEPR shrinks as the covering radius of the original code decreases.

For $h = 1$ and $h = 2$ we exhibited examples where the lower bound in Theorem 2 is attained. Theorem 2 was also employed to show that most phase-shift designs from the literature are (nearly) optimal. It was demonstrated as well that for several code families of practical importance, including BCH codes and convolutional codes, a significant PMEPR reduction is ruled out by Theorem 2.

We close with a discussion of some open problems and possible further research directions suggested by our work.

We have identified codes for which the lower bound on the PMEPR is asymptotically independent of the length of the code. Namely these are the duals of the binary primitive BCH codes and Reed–Muller codes. Indeed Davis and Jedwab [9] constructed $m!/2$ cosets of the first-order Reed–Muller code, $\mathrm{RM}(1, m)$, with PMEPR at most $2$. We ask: do there exist cosets of arbitrary Reed–Muller codes whose PMEPR is upper bounded by a constant? If so, find a way to construct them.

We have analyzed lower bounds on the expression in (3). Although such a bound can be used to rule out significant PMEPR reductions in certain cases, the bound does not claim the existence of $2^h$-ary codes equivalent to binary codes whose PMEPR is equal to or close to this bound. Therefore it would be interesting to find a good upper bound for (3). Such a bound could provide results on the existence of good phase shifts.

Finally we wish to restate the most essential (and most difficult) open problem within this context. Given $h$ and a binary code $\mathcal{B} \subseteq \mathbb{Z}_2^n$, find a code in $E_h(\mathcal{B})$ whose PMEPR is equal to the value in (3).

## References


[1] E. R. Berlekamp and L. R. Welch, "Weight distributions of the cosets of the (32,6) Reed–Muller code," *IEEE Trans. Inf. Theory*, vol. 18, no. 1, pp. 203–207, Jan. 1972.

[2] I. E. Bocharova and B. D. Kudryashov, "On the covering radius of convolutional codes," in *Proc. First French-Israeli Workshop (Lecture Notes in Computer Science)*, vol. 781. Berlin, Germany: Springer-Verlag, 1993, pp. 56–62.

[3] R. Brualdi, S. Litsyn, and V. Pless, "Covering radius," in *Handbook of Coding Theory*, V. S. Pless and W. C. Huffman, Eds. Elsevier, 1998.

[4] A. R. Calderbank, P. C. Fishburn, and A. Rabinovich, "Covering properties of convolutional codes and associated lattices," *IEEE Trans. Inf. Theory*, vol. 41, no. 3, pp. 732–746, May 1995.

[5] C. Carlet, "$\mathbb{Z}_{2^k}$-linear codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 4, pp. 1543–1547, Jul. 1998.

[6] C. Carlet and S. Mesnager, "Improving the upper bounds on the covering radii of binary Reed–Muller codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 162–173, Jan. 2007.

[7] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein, *Covering Codes*. Amsterdam, The Netherlands: Elsevier, 1997.

[8] S. D. Cohen, "The length of primitive BCH codes with minimal covering radius," *Designs, Codes and Cryptography*, vol. 10, no. 1, pp. 5–16, Jan. 1997.

[9] J. A. Davis and J. Jedwab, "Peak-to-mean power control in OFDM, Golay complementary sequences, and Reed–Muller codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2397–2417, Nov. 1999.

[10] *Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Physical (PHY) Layer, document RTS0023003-R2*, European Telecommunications Standards Institute (ETSI), Sophia-Antipolis, Valbonne, France, Feb. 2001.

[11] D. Gorenstein, W. Peterson, and N. Zierler, "Two-error correcting Bose-Chaudhuri codes are quasi-perfect," *Information and Control*, vol. 3, pp. 291–294, 1960.

[12] T. Helleseth, "All binary 3-error-correcting BCH codes of length $2^m - 1$ have covering radius 5," *IEEE Trans. Inf. Theory*, vol. 24, no. 2, pp. 257–258, Mar. 1978.

[13] T. Helleseth, T. Kløve, and J. Mykkeltveit, "On the covering radius of binary codes," *IEEE Trans. Inf. Theory*, vol. 24, no. 5, pp. 627–628, Sep. 1978.

[14] H. Janwa, "Some new upper bounds on the covering radius of binary linear codes," *IEEE Trans. Inf. Theory*, vol. 35, no. 1, pp. 110–122, Jan. 1989.

[15] A. E. Jones and T. A. Wilkinson, "Combined coding for error control and increased robustness to system nonlinearities in OFDM," *Proc. of IEEE 46th Vehicular Technology Conf. (VTC), Atlanta, GA*, pp. 904–908, Apr. 1996.

[16] A. E. Jones, T. A. Wilkinson, and S. K. Barton, "Block coding scheme for reduction of peak to mean envelope power ratio of multicarrier transmission schemes," *IEE Electron. Lett.*, vol. 30, no. 25, pp. 2098–2099, Dec. 1994.

[17] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.

[18] A. M. McLoughlin, "The complexity of computing the covering radius of a code," *IEEE Trans. Inf. Theory*, vol. 30, no. 6, pp. 800–804, Nov. 1984.

[19] J. Mykkeltveit, "The covering radius of the (128,8) Reed–Muller code is 56," *IEEE Trans. Inf. Theory*, vol. 26, no. 3, pp. 359–362, May 1980.

[20] D. J. Newman, "An $L^1$ extremal problem for polynomials," *Proc. Amer. Math. Soc.*, vol. 16, pp. 1287–1290, Dec. 1965.

[21] K. G. Paterson, "Generalized Reed–Muller codes and power control in OFDM modulation," *IEEE Trans. Inf. Theory*, vol. 46, no. 1, pp. 104–120, Jan. 2000.

[22] K. G. Paterson and V. Tarokh, "On the existence and construction of good codes with low peak-to-average power ratios," *IEEE Trans. Inf. Theory*, vol. 46, no. 6, pp. 1974–1987, Sep. 2000.

[23] K.-U. Schmidt, "On cosets of the generalized first-order Reed–Muller code with low PMEPR," *IEEE Trans. Inf. Theory*, vol. 52, no. 7, pp. 3220–3232, Jul. 2006.

[24] ——, "Complementary sets, generalized Reed–Muller codes, and power control for OFDM," *IEEE Trans. Inf. Theory*, vol. 53, no. 2, pp. 808–814, Feb. 2007.

[25] M. Sharif and B. Hassibi, "Existence of codes with constant PMEPR and related design," *IEEE Trans. Signal Proces.*, vol. 52, no. 10, pp. 2836–2846, Oct. 2004.

[26] V. Tarokh and H. Jafarkhani, "On the computation and reduction of the peak-to-average power ratio in multicarrier communications," *IEEE Trans. Commun.*, vol. 48, no. 1, pp. 37–44, Jan. 2000.

[27] A. A. Tietäväinen, "An upper bound on the covering radius as a function of the dual distance," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1472–1474, Nov. 1990.

[28] S. G. Vladuts and A. N. Skorobogatov, "Covering radius for long BCH codes," *Probl. Pered. Inf.*, vol. 25, pp. 38–45, 1989, translated in Probl. Inf. Transm., vol. 25, no. 1, pp. 28-34, 1989.

[29] G. Wunder and H. Boche, "A baseband model for computing the PAPR in OFDM systems," *Proc. of 4th Int. Conf. Source and Channel Coding, Berlin, Germany*, pp. 273–280, Jan. 2002.